UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,391	07/26/2001	Neil John Hursey	01.059.01	5033

7590 09/23/2009

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
09/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte NEIL JOHN HURSEY and WILLIAM ALEXANDER MCEWAN

Appeal 2008-005953
Application 09/912,391
Technology Center 2400

Decided: September 23, 2009

Before JAMES D. THOMAS, LANCE LEONARD BARRY, and DEBRA K. STEPHENS, *Administrative Patent Judges*.

THOMAS, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1-4, 6 -12, 14 -20, and 22 -28. Appellants have canceled claims 5, 13, and 21. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Invention

> An e-mail client serves to detect mass mailing malware by detecting if over a threshold number of addressees from within the address book of that e-mail client are being sent an e-mail or over a predetermined number of substantially identical e-mails are being sent by that e-mail client. The sending of e-mail messages to a substantial proportion of the addressees within an address book is a characteristic indicative of mass mailing malware. A quarantine queue may be provided in which e-mail messages are held for a predetermined period prior to being sent out in order that separate e-mail messages being sent to a large proportion of the address book addressees may be identified and linked together.

(Spec. 16, Abstract, Figs. 3-5.)

Representative Claim

9. A method of detecting e-mail propagated malware within an email client computer, said method comprising the steps of:

generating an e-mail message;

comparing said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer;

identifying whether;

(i) said e-mail message is being sent to more than a threshold number of addresses specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addresses specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said email message is identified as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and

holding said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer.

Prior Art and Examiner's Rejections

The Examiner relies on the following references as evidence of unpatentability:

Kouznetsov	6,725,377 B1	Apr. 20, 2004 (filed March 12, 1999)
Marsh	6,763,462 B1	July 13, 2004 (filed Oct. 5, 1999)
Radatii	6,763,467 B1	July 13, 2004 (filed Feb. 3, 1999)
Bates	6,779,021 B1	Aug, 17, 2004 (filed July 28, 2000)
Bates ("Bates 2")	6,785,732 B1	Aug. 31, 2004 (filed Sept. 11, 2000)

All claims on appeal 1 through 4, 6 through 12, 14 through 20, and 22 through 28 stand rejected under the written description portion of 35 U.S.C. § 112, first paragraph. These claims also stand rejected under 35 U.S.C. § 103. In a first stated rejection, the Examiner relies upon Bates in view of Marsh as to claims 1-3, 7, 9-11, 15, 17-19, 23, and 26. In the second stated rejection, the Examiner adds Bates 2 to reject claims 4, 6, 12, 14, 20, 22, 27, and 28. The Examiner adds Kouznetsov to the combination of Bates and Marsh in the third stated rejection under 35 U.S.C. § 103 as to claims 8, 16, and 24. Lastly, the Examiner further relies upon Radatii in addition to the combination of Bates and Marsh as to claim 25 in a fourth stated rejection.

Claim Groupings

Based upon Appellants' arguments in the principal Brief on appeal, we will utilize independent claim 9 as representative of the subject matter of independent claims 1, 9, and 17 as to the rejection under 35 U.S.C. § 112, first paragraph, and for the initial rejection under 35 U.S.C. § 103. Separate arguments are represented in the principal Brief only as to dependent claims, 25 -28. We will address the subject matter of them separately. It is noted that the rejection under 35 U.S.C. § 103 utilizing Kouznetsov has not been separately argued and appellants rely for patentability upon the arguments presented as to the respective parent independent claims, of which we consider independent claim 9 as representative.

ISSUES

1. Have Appellants shown that the Examiner erred in finding lack of support for certain enumerated subject matter set forth in representative independent claim 9 on appeal?

2. Have Appellants shown that the Examiner erred in finding that the respective combination of references teaches or suggests that subject matter of representative independent claim 9 and dependent claims 25 through 28?

FINDINGS OF FACT ("FF")

1. Appellants describe the state of the prior art in part:

> Some of the most prolific and damaging computer viruses in recent times have replicated and distributed themselves by use of the victim's e-mail service. The virus is received in an e-mail and when activated serves to replicate and send itself to most, if not all, of the e-mail addresses listed in the victim's e-mail

> address book. The infected e-mail is then received by another unsuspecting user who again causes it to replicate it propagate.

(Spec. 2, ll. 10-15.)

2. On the one hand, while the title of the invention to the Bates patent relates to a method and system for predicting and managing undesirable electronic mail, its Abstract appears to focus upon approaches taken only within a server. On the other hand, there are significant teachings in this patent relating to methodologies that correspond to actions within a client as well as we will note in turn.

At column 1, lines 21-26, Bates states:

> A client is typically a requester of services, and a server is the provider of services. A single machine can be both a client and a server depending on the software configuration. A typical client machine is loaded with client software, while a typical server machine is loaded with server software.

With respect to Figure 1, column 5, lines 18-21 state: "a computer system that may be utilized as a stand-alone computer system or one of the clients or servers on a network is presented." Figure 2 shows a system arrangement, and Figure 3 shows the software modules associated with the network server 40. Figure 5 shows a client system 60 from the block showing in Figure 2, where Figure 5 also identifies various software modules within the client system itself. Figure 6 illustrates client displays relative to the logic associated with determining spam including illustrations of percentages associated with the determination of whether or not spam exists. Figure 7 shows the management of e-mail at a client, which compares with the showing in Figure 4B, item D beginning with flow chart element 130 that associates client actions with respect to server activities as well.

The paragraph bridging columns 1 and 2 updates and discusses the receipt and sending of unsolicited e-mail, which states that such mail may include viruses, worms or other destructive attachments that can easily be transmitted within a server upon activation at a single client. Furthermore, the sentence bridging column 7 and 8 indicates that received e-mail may have embedded HTML links that may be associated with spam.

The logic of Figure 4A relates to processes that predict undesirable email. They include comparing new email with previously confirmed email spam, addresses, titles, and keywords as well as determinations of thresholds or percentages of recipients of email greater than a designated number of recipients, such as those illustrated in Figure 6 noted earlier. These determinations relate to the functionalities associated with the first column of flow chart Figure 4A, where those in the latter portion of the second column, beginning with logic block 110, relate to determinations of substantial similarities, such as by size and content as well in an effort to identify received email as spam. The first column of flow chart 4B illustrates the determination by updating email histories and spam rules according to the software functionalities and modules illustrated in Figure 3.

With respect to the server architecture showing at Figure 3, Bates teaches at column 6, lines 49-50, that "E-mail folder 44 preferably provides storage of all incoming and outgoing e-mails according to user account." In a corresponding client showing in Figure 5, "E-mail data base 66 preferably temporarily holds a copy of the users' e-mail folder accessed from the network server" as discussed at column 11, lines 16-18. According to the operability of a mail organizer application 62 in Figure 5, users and corporations or administrators may establish spam handling rules as

discussed beginning at column 11, line 33, and "a user may designate a preference in user preferences 64 for all predicted spam to be automatically moved to a trash folder if a user does not open the predicted spam after a first session being displayed" as discussed at column 11, lines 49-52.

In addition to these complementary storage areas in the client in server in Bates, this reference significantly teaches the following at column 6, lines 64-column 7, line 12:

> As an additional feature, prediction application 42 may also analyze out-going e-mail in the same manner as in-coming e-mail to predict the likelihood of each outgoing e-mail as spam. Thereby, a corporation or other provider that hosts network server 40 may utilize spam prediction filters to detect out-going spam and further restrict employees or other users from utilizing e-mail accounts to transmit spam. This feature is particularly helpful in subduing the spread of viruses, such as those that automatically transmit themselves utilizing client e-mail address books.
>
> Multiple levels of prediction may be determined by prediction application 42. For example, a percentage of likelihood as spam may be determined by prediction application 42. In another example, prediction application 42 may predict that a particular e-mail is in a particular category of spam, such as viral, job marketing, pornographic, etc.

The functionality associated with the prediction application 42 in Figure 3 also includes the following teachings at column 7, lines 22 through 29:

> In a preferred embodiment, during the first filtering process, prediction application 42 looks for an unusually large number of users receiving the same e-mail from a particular user address in a given time period. For example, if more than five percent of users receive an e-mail from a particular user address

> within one minute, then prediction application 42 may predict that the e-mail is spam.

Column 8, lines 7 through 10, also teaches that "spam data base 46 may contain a history of all e-mails sent to and received from network server 40 in a database format that can be searched according to sender, recipient, title content, etc. in a manner that is time-saving."

3. The title of Marsh's patent relates as well to e-mail virus detection utilities that focus upon e-mail addresses in a distribution list or electronic address book that relates to client operations as revealed in the Abstract of this patent. The background of Marsh at column 1 indicates that it was known in the art that computer viruses can spread through electronic mail and specifically teaches at lines 32-35 that "a virus may attempt to send a copy of itself to other computers by sending e-mail messages including destructive code segments." Thus, an artisan would appreciate that Marsh relates to outgoing electronic mail messages.

The system 100 in Figure 1 of Marsh illustrates email application 102 and a virus utility 104 that examines email distribution patterns.

Figure 2 of Marsh shows a flow diagram of a virus detection utility that includes inspecting outgoing messages 202 and comparing email addresses with potential recipients in block 204. For selected addresses identified as recipients, the users are notified in element 208. More significantly, Marsh teaches at column 3, lines 35-65:

> A user may be notified of possible virus activity (block 208) through any conventional messaging technique such as a pop-up warning dialog. A virus warning may include information regarding recent e-mail activity such as recipients and message content. The virus warning may also give a user options to respond to possible virus activity including deleting an

> outgoing message without sending, saving an outgoing message for later examination, or disregarding the warning and sending an outgoing message.
> In yet another embodiment, the virus detection utility 104 may examine e-mail distribution patterns to determine if a computer virus is replicating itself by sending e-mail messages to individual e-mail addresses (i.e., one at a time). Some viruses may attempt to send a series of e-mail messages, each to a different e-mail address, in an effort to disguise a mass distribution of virus code segments. The random numbers generated may again represent positions of an e-mail addresses in a distribution list or address book. In this embodiment, the virus detection utility 104 may track e-mail messages sent by the e-mail application 102. If electronic messages are sent to each of the e-mail addresses represented by the random numbers in a specified period of time, a virus warning may be issued to a user. The user would again have the options described above regarding the disposition
> of an outgoing message. For example, if e-mail messages are transmitted to all recipients identified by the random numbers within two minutes, a user may be alerted. Alternatively, potential virus activity may be identified if electronic messages are transmitted to a particular number of the selected e-mail addresses (e.g., 3 out of 5) within the specified period of time, e.g. two minutes.

4. Like the initial Bates patent, Bates 2 contains complementary teachings relating to virus checking methodologies in servers and clients. Initially, Bates 2 teaches at column 1, lines 46-53:

> Virus checking application programs are currently available for checking viruses on individual computers. Norton Anti-virus and McAfee VirusScan are two examples of commercially-available virus checkers. Known virus checkers run on a single computer system, such as a web server or a web client. These virus checkers typically are run at the user's request to determine whether there are any viruses on any specified drive or file.

The ability of users to set preferences is illustrated in Figure 6 and discussed beginning at column 8, line 45.

The initial showings in Figures 1 and 3 relate to server activities. Email virus processing activities are illustrated in Figure 7 to include checking attachments for viruses. Figure 10 illustrates the ability of a user/client to download virus checking software in a corresponding manner.

In the paragraph bridging column 7 and 8, Figure 4 is discussed to include the notification determination of a virus being found. This action includes the following teachings at column 8, lines 15-22:

> Finally, the appropriate authorities may be notified of the virus (step 470). The term "appropriate authorities" is a broad term that encompasses anyone who may need to know about the occurrence of a virus, including a network administrator of a local area network, a web site administrator, a contact person in a virus detection company, and appropriate law enforcement officials, such as local, state, federal, and international law enforcement agencies.

5. Radatti's background of the invention discusses at column 1, lines 36-48 the following:

> Virus, worms, and trojan horses can infect an internal network or single computer system when the internal network or computer system executes a program from the external network that contains the hostile algorithm. All binary executables, unreviewed shell scripts, and source code accessed from an external network may contain worms, viruses, or trojan horses. In addition, outside binary executables, shell scripts, and scanned source code may enter en internal network or single computer system through an E-mail attachment. Also, executables can be directly accessed from an external network through the IFTP program, a world-wide web browser, or an outside contractor whose network already has been compromised.

PRINCIPLES OF LAW

Obviousness

"[T]he PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000)). "Moreover, limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (citing *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989)). Our reviewing court has repeatedly warned against confining the claims to specific embodiments described in the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc).

One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

> Section 103 forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 406 (2007).

The Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," and discussed circumstances in which a patent might be determined to be obvious. *Id.* at 415 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 13-14 (1966)). The Court reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* at 416. The operative question in this "functional approach" is thus "whether the

improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 415, 417.

We must determine whether or not the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *See id.* at 407. Obviousness determination is not the result of a rigid formula, and we will consider the facts of a case and the common sense of those skilled in the art. *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161 (Fed. Cir. 2007) (citation omitted). That is, the test for obviousness is rather what the combined teachings of the references would have suggested to those of ordinary skill in the art. *See In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991); *In re Keller*, 642 F.2d 413, 425 (CCPA 1981).

Teaching Away

As to the specific question of "teaching away," our reviewing court in *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994) stated "[a] reference may be said to teach away when a person of ordinary skill, upon [examining] the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." (citation omitted).

ANALYSIS

1. Rejection under the written description portion of the first paragraph of 35 U.S.C. § 112

With respect to the written description rejection, the Examiner states at page 3 of the Answer: "although there is support for each of (i), (ii) and (iii) in the alternative, as shown in page 7 line 30-page 8 line 15 of the present specification, but never as a combination." The Examiner persists in this view at page 9 of the Answer by continuing to urge that there is no "support for identifying all of (i), (ii), and (iii) together. Rather, the section of the specification which supports (i), (ii), (iii) located at Page 7 Line 30-Page 8 Line 15, only supports identification of these conditions in the alternative."

With respect to the subject matter actually recited in representative independent claim 9, the identification is recited to occur "whether" the three enumerated items identified by the Examiner are present. The second and third items are connected by the connective "and." This recitation is akin to a Markush grouping common in the chemical arts. Significantly, the claim additionally recites "wherein said email message is identified as potentially containing malware if at least one of items (i), (ii), and (iii) is identified."

The Examiner misperceives the actual, minimal requirements of the independent claims on appeal to include the capability that all are required at the same time. By its own terms, the claim merely requires "at least one of" the three items listed to be identified, which is consistent with the use of the word "whether" earlier in the claim.

As noted by Appellants' briefing before us, Specification page 2, line 30-page 3, line 14 as originally filed indicates corresponding limitations to those presently claimed to include the recitation of "identifying logic operable to identify said e-mail message as potentially containing malware if

at least one of" which recites the three enumerated circumstances. This language is also recited in original independent claims 1, 9, and 17. Since the Examiner recognizes that the disclosure originally filed indicates the three contingent elements are set forth in the alternative, and because they are still claimed in the alternative, the Examiner's rejection of all claims on appeal under the written description portion of 35 U.S.C. § 112, first paragraph, is reversed. Appellants' briefing has shown error in the Examiner's positions as to this rejection.

2. Rejections under 35 U.S.C. § 103

At the outset, we address Appellants' apparent arguments that Bates and Marsh are not properly combinable within 35 U.S.C. § 103. We strongly disagree with this view since Examiner's choice and identification of teachings of Marsh and Bates, further buttressed by FF 2 and 3, are consistent with the governing case law set forth earlier in this opinion. The artisan would well understand that the combination of teachings relied upon among these two references relates to a combination of familiar elements utilizing known methods to yield predictable results according to their established functions. Our extensive citation of the pertinent teachings in Bates and Marsh in FF 2 and 3 would also clearly indicate that the artisan would understand that Bates teaches features associated with clients and servers in addition to Marsh's predominant teachings relating to clients only. We have indicated that Bates 2 even contains similar overlapping teachings relating to clients as well as servers in FF4.

We have considered in detail Appellants' arguments regarding an alleged teaching away of the combination of Bates and Marsh in the Brief

and the Reply Brief. The bulk of these arguments relate to the features that are not necessary to be present among the references, such as the elements recited in the alternative associated with the identified sub clauses of representative independent claim 9 on appeal, (ii), and (iii). Again, the teachings we and the Examiner have identified with respect to Bates and Marsh clearly indicate the combinability of them within 35 U.S.C. § 103 from an artisan's perspective. Moreover, according to the guidance provided by the earlier-noted case law, Appellants have not shown to us that either or both of these references would have discouraged the artisan from following the path set out between them or would be led in a direction divergent from the path actually taken by Appellants.

In other words, their teachings clearly indicate the obviousness of the paths taken by appellants. The artisan would clearly consider the teachings of Marsh and Bates complementary and thus aid in their combinability.

Problems associated with emails that include viruses being received by a client that can be activated and replicated to addressees using a client's email address book were identified by Appellants' as known in the art in FF 1. We have identified corresponding teachings with respect to various storage capabilities in Bates to include the identification in a corresponding manner of viruses received in the address books of clients in the quoted material we reproduced in FF 2, at columns 6 and 7 of Bates. With the other teachings related to so-called executables we identified in FF 2 in Bates and the just noted the teachings of the ability of viruses to automatically transmit themselves utilizing clients' email address books, the artisan would understand that the complementary teachings already exist as well in Marsh as we have identified in FF 3. These teachings are in addition to those

already relied upon by the Examiner as to claim 25 and the teachings of executables well known in the art in FF 5 in Radatti.

The Examiner's reliance upon Bates' teachings at column 8, line 56-column 9, line 2 relates to the showings in the Figure 4A of this reference that we have discussed in brief in FF 2 and clearly pertain to the initial alternative recitation "(i) said e-mail messages being sent to more than a threshold number of addresses specified within said address book." The showings in Figures 4A, 4B, and 7 of Bates clearly relate to such a threshold determination, which is taught to even include the claimed "a threshold number," which is broad enough to include only one.

We identified in FFs 2 and 3 pertinent teachings in both Bates and Marsh relating to the claimed feature of temporarily storing, as in the claimed a quarantine queue, for a period prior to being sent from the computer for respective messages as recited at the end of representative independent claim 9 on appeal. These include the teachings at column 7, lines 22 -29 of Bates and part of the extensive quoted material from column 3 of Marsh.

As to dependent claim 26, we find that the mere sharing of common attachments among previously generated and currently generated email messages was contemplated by the extensive citation of noted teachings in FF 2 relating to Bates alone, notwithstanding the additional teachings the Examiner has isolated and we have noted in FF 3 in Marsh. The Examiner and we noted from the paragraph bridging columns 1 and 2 of Bates in FF 2 the detailed teachings of logic in Figures 4A, 4B, and 7 of Bates regarding emails based upon the known property of e-mails having attachments that may include destructive viruses.

The Examiner's additional reliance upon Bates 2 in the second stated rejection under 35 U.S.C. § 103 pertains to argued dependent claims 27 and 28. Notifying the provider or sender of the identified malware in dependent claim 27 would have been an obvious variation among the broad teachings we identified in FF 4 associated with the teachings at column 8 of Bates 2. The teachings include anyone who may need to know about the occurrence of such virus, which obviously would have included the sender. Additionally, the Examiner's use of common sense in the art as to sending a copy of the actual originating email in the message to this provider, as recited in the dependent claim 28, is also considered to have been an obvious additional function as the Examiner argues in light of the earlier-noted case law when taken from the perspective of the person of ordinary skill in the art.

Appellants do not argue that Bates 2 is not properly combinable within 35 U.S.C. § 103 to the combination of Bates and Marsh as to the second stated rejection under 35 U.S.C. § 103. The Examiner further relies upon Kouznetsov in the third stated rejection under this statutory basis. Appellants rely for patentability upon the features already argued with respect to the first stated rejection that includes representative independent claim 9 on appeal. Again, Appellants do not argue that this reference is not properly combinable with the combination of Bates and Marsh.

We have already addressed the fourth stated rejection under 35 U.S.C. § 103 of dependent claim 25 regarding the teachings of Radatti with respect to our earlier discussion relating to the receipt of email messages in address books and the extensive realization among the prior art relied upon that malware in the form of separate executable elements of dependent claim 25

were known to be part of received email messages. Again, Appellants did not separately argue Radatti is not properly combinable within 35 U.S.C. § 103 to combination of Marsh and Bates.

Because we have found that the Examiner has provided substantial evidence of unpatentability of all argued claims on appeal among the plurality of references that are properly combinable within 35 U.S.C. § 103, Appellants' arguments in the Brief and Reply Brief are considered not persuasive of patentability. Appellants' reproduction of all of the arguments presented the principal Brief on appeal and the Reply Brief, in addition to the responsive arguments in the Reply Brief to the Examiner's responsive arguments in the Answer, is not helpful to us and is not required by the rules.

CONCLUSIONS OF LAW

1. Appellants have shown that the Examiner erred in finding that certain presently claimed features in representative independent claim 9 on appeal are without proper written description support within the first paragraph of the 35 U.S.C. § 112.

2. On the other hand, Appellants have not shown that the Examiner erred in finding that the respective combinations of teachings of the references among each of the four separately stated rejections under 35 U.S.C. § 103 would have rendered obvious the correspondingly rejected claims.

DECISION

The Examiner's rejection under the written description portion of the first paragraph of 35 U.S.C. § 112 of all claims on appeal, claims 1 through 4, 6 through 12, 14 through 20, and 22 through 28, is reversed. The

Examiner's separate rejections of all of these claims under 35 U.S.C. § 103 are affirmed. Since we have affirmed rejections encompassing all claims on appeal, the decision of the Examiner is affirmed. All claims on appeal are unpatentable.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED

erc

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120